IN THE SPECIFICATION:

Please replace the paragraph beginning on page 1, line 10 of the specification and ending at page 2, line 10 of the specification with the following:

The Internet provides users with convenient and ubiquitous access to digital content. Because of the potential of the Internet as a powerful distribution channel, many CE products strive to interoperate with the PC platform — the predominant portal to the Internet. The use of the Internet as a distribution medium for copyrighted content creates the compelling challenge to secure the interests of the content provider. In particular it is required to warrant the copyrights and business models of the content providers. Control of the playback software is one way to enforce the interests of the content owner including the terms and conditions under which the content may be used. In particular for the PC platform, the user must be assumed to have complete control to the hardware and software that provides access to the content and unlimited amount of time and resources to attack and bypass any content protection mechanisms. As a consequence, content providers must deliver content to legitimate users across a hostile network to a community where not all users can be trusted. The general approach in digital rights management for protected content distributed to PCs is to encrypt the digital content (for instance using DES) and to store the decryption key (or the "license") in a so-called License database on the PC's hard disk. Digital content on the PC is typically rendered using media players, such as Microsoft's Media Player, Real's RealOne Player, Apple's QuickTime player. Such players can load for a specific content format a respective plug-in for performing the format-specific decoding. Those content formats may include AVI, DV, Motion JPEG, MPEG-1, MPEG-2, MPEG-4, WMV, Audio CD, MP3, WMA, WAV, AIFF/AIFC, AU, etc. The player and plug-in

structure is illustrated in Fig. 1, where a media player 100 includes a core player 110 and several format-specific plug-ins (shown are plug-ins 120, 122 and 124). The core player 110 may, for example, provide the user interface for controlling the player. Each plug-in includes a respective decoder. It may send the decoded content directly to rendering HW/SW, such as a sound-card, or pass it on to the core player 110 for further processing. For secure rendering, a secure plug-in is used that not only decodes the content in the specific format but also decrypts the content. This is illustrated in Fig.2, where the encrypted content is first fed through a decryptor 230 and next the decrypted content is fed through the format-specific decoder 220. The decryptor 230 may receive a decryption key/license from a license database 210.